UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

KAVON FORD, individually and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

EMPRESS AMBULANCE SERVICE LLC D/B/A EMPRESS EMS;

Defendant.

Case No. _____

CLASS ACTION

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Kavon Ford ("Plaintiff"), on behalf of himself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against the above-captioned Defendant, Empress Ambulance Service LLC d/b/a Empress EMS ("Defendant") upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

I. NATURE OF THE ACTION

1. Plaintiff Ford brings this Action against Empress EMS, an emergency medical services and aftercare transportation provider in New York state, for its failure to safeguard his and approximately 318,558 other individuals' private and confidential information, including their names, dates of service, Social Security numbers, and insurance information ("PII").

2. Specifically, this Action arises from a data breach whereby unauthorized, third-party actors gained access to Defendant's network on May 26, 2022. Defendant did not detect this unauthorized access until July 14, 2022 – but at that point, nearly two months had passed since this unauthorized access had initially occurred and, in that time, the hackers had unfettered access to Defendant's network, including encrypted portions of it (the "Data Breach). The hackers "copied a small subset of files on July 13, 2022" according to Defendant's *Notice of Data Breach* (the "*Notice*"); however, this is a gross understatement of what actually occurred: the negligent compromise of nearly 1/3rd of a million people's most sensitive PII.

3. The *Notice* was also disseminated late (there is a two-month gap between when the files were copied and when the *Notice* letter was issued); additionally, the *Notice* fails to state whether Defendant ever regained control of its network or how the intrusion occurred in the first place. The Defendant likely knows all of this vital information as a result of its "thorough investigation" of the incident but fails to inform victims of the full picture of what occurred with respect to this particular Data Breach. As a result of this inadequate and delayed response, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at present and continuing risk of identity theft and various other forms of personal, social, and financial harm.

4. Plaintiff and Class Members' unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions, and due to its utter failure to protect Class Members' sensitive data. Hackers targeted and obtained victims' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The risks to these persons will remain for their respective lifetimes.

5. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include, but are not limited to: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (v) charges and fees associated with fraudulent charges on their accounts, and (vi) the continued and certainly an increased risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

6. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or at the very least negligently failing to take and implement adequate and reasonable measures to ensure that its customers' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to damages, injunctive and other equitable relief.

II. PARTIES

Plaintiff Kavon Ford

7. Plaintiff Ford is a New York resident. He provided his PII to Empress in connection with receiving healthcare services from Empress. He received a letter from Empress on or about September 9, 2022 notifying him that his PII may have been exposed in the Data Breach as alleged herein.

Defendant Empress Ambulance Service LLC d/b/a Empress EMS

8. Defendant Empress Ambulance Services LLC d/b/a Empress EMS is a Delaware corporation with its principal place of business located in Yonkers, New York.

III. JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332 (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00), there is diversity of citizenship between at least one class member and the Defendant and this is a class action involving 100 or more class members.

10. This Court has personal jurisdiction over Empress EMS because Empress EMS is a limited liability company organized under the laws of Delaware and has its principal place of business at 722 Nepperhan Ave, Yonkers, New York, 10703.

11. Venue properly lies in this judicial district pursuant to 28 U.S.C. § 1391 because, *inter alia,* the events or omissions giving rise to the conduct alleged herein occurred in, were directed to, and/or emanated from this district; Defendant's principal place of business is in this district; Defendant transacts substantial business and has agents in this district; a substantial part

of the conduct giving rise to Plaintiff's claims occurred in this judicial district; and because Plaintiff resides within this district.

IV. FACTUAL ALLEGATIONS

Defendant's Business

12. According to Defendant, Empress EMS is "one of the largest, most experienced emergency and non-emergency response providers in Westchester, Rockland, Ulster, Dutchess, Putnam, Orange County, and the Bronx, New York."[1] Defendant purports to have over 700 employees and a 24-hour communications center "[h]ousing one of the most advanced computer aided systems in the region."[2]

13. Defendant understands the need to protect the data it collects and according to the Defendant's Privacy Policy:

> Empress Ambulance Service, LLC is committed to protecting your personal health information. We are required by law to maintain the privacy of health information that could reasonably be used to identify you, known as "protected health information" or "PHI." We are also required by law to provide you with the attached detailed Notice of Privacy Practices ("Notice") explaining our legal duties and privacy practices with respect to your PHI.
>
> We respect your privacy, and treat all healthcare information about our patients with care under strict policies of confidentiality that our staff is committed to following at all times.

14. Within the scope of administering healthcare to customers, mainly through transporting them to and from the hospital in ambulances, Defendant collects a significant amount of both PII and PHI. This includes, but is not limited to, the PII which was compromised in the Data Breach as alleged herein.

[1] https://empressems.com, (last accessed Oct. 10, 2022).
[2] *Id.*

15. Defendant agreed to and undertook legal duties to maintain the PII entrusted to it by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

16. The information held by Defendant in its computer system and network included the PII of Plaintiff and Class Members. Defendant voluntarily assumed custody of Plaintiff's and Class members' PII for its own profit. Defendant was aware of its obligations as demonstrated by its Privacy Policy.

17. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure, as in the targeted Data Breach here.

18. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

19. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

The Data Breach

20. **T**his Action arises from a targeted cyberattack in which unauthorized, third-party actors gained access to Defendant's network on May 26, 2022. Defendant did not detect this unauthorized access until July 14, 2022 – but at that point, nearly two months had passed since this unauthorized access had initially occurred and, in that time, the hackers had unfettered access within Defendant's network including encrypted portions of it during that timespan and acquired hundreds of thousands of people's most sensitive PII.

21. Additionally, according to a data breach reporting website, databreaches.net, Hive, a notorious ransomware hacking group was not only responsible for the Data Breach as alleged herein and had communications with Empress after downloading data contained on Defendant's servers. Hive's note to Empress on July 14, 2022, in-part, reads as follows:

> ! ! ! DO NOT TRY TO DECRYPT OR CHANGE ENCRYPTED FILES ON YOUR COMPUTERS, IT WILL COMPLETELY DESTROY THEM ! ! !
>
> Ladies and gentlemen! Attention, please! This is HIVE ransomware team. We infiltrated your network and stayed there for 12 days (it was enough to study all your documentation and gain access to your files and services), encrypted your servers.
>
> Downloaded most important information with a total size over 280 GB.
>
> Few details about information we have downloaded: – contracts, nda and other agreements documents – company private info (budgets, plans, investments, company bank statements, etc.) – employees info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.) – customers info (SSN numbers, emails, addresses, passports, phone numbers, payments, working hours, etc.) – SQL databases with reports, business data, customers data, etc. – approximate number of personal records including addresses and ssn's data is above 10000 units.

22. Hive then contacted Empress again on July 15, 2022 with a sample of the files that were exfiltrated in the Data Breach; some of the files that were offered contained not only the PII as alleged herein, but also protected health information ("PHI") of Defendant's patients.

23. By no means was this Data Breach merely "a small subset of files" being compromised – it was a calculated, targeted highly sophisticated ransomware attack perpetrated by a complex, notorious ransomware hacking group which downloaded and exposed a massive amount of PII.

24. And not only was the Defendant's underplaying of the incident in the *Notice* a major glaring issue, but the *Notice* was also disseminated late (there is a two month gap between when the files were copied and when the *Notice* letter was issued); additionally, the *Notice* fails to state whether the Defendant ever regained control of its network as well as how the intrusion occurred in the first place. As a result of this inadequate and delayed response, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at present and continuing risk of identity theft and various other forms of personal, social, and financial harm.

25. Upon information and belief, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the PII of patients like Plaintiff and the Class Members.

26. Because of the Defendant's failure to properly safeguard Plaintiff's and Class Members' PII, data thieves were able to gain unauthorized access to Defendant's IT systems and were able to compromise, access, and acquire the unprotected PII of Plaintiff and Class Members.

27. Defendant had obligations created by industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their PII confidential and to protect it from unauthorized access and disclosure.

28. Defendant's data security obligations were particularly important and should have been apparent given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

29. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[3] Of the 1,862 recorded

[3] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[4] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[5]

30. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC Health System (286,876 patients, March 2020), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

31. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[6]

32. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[7]

33. The ransomware attack at issue is a readily foreseeable threat to businesses like Defendant. A ransomware attack is a type of cyberattack that is frequently used to target healthcare

[4] *Id.*
[5] *Id.*
[6] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Jan. 25, 2022).
[7] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

providers due to the sensitive patient data they maintain.[8] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[9] Ransomware attacks are particularly harmful for patients and healthcare providers alike as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates.[10] In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.[11]

34. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[12] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

35. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[13] In 2020, over 50% of ransomware attackers exfiltrated data from a network

[8] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/
[9] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs
[10] *Ponemon study finds link between ransomware, increased mortality rate*, available at https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate
[11] *The State of Ransomware in Healthcare 2022*, available at https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf
[12] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends
[13] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

before encrypting it.[14] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[15] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[16]

36. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Fails to Comply with FTC Guidelines

37. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

38. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone

[14] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report
[15] *Id.*
[16] *Id.*
[17] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 15, 2021).

is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

39. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

41. These FTC enforcement actions include actions against healthcare related providers like Defendant. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

42. Defendant failed to properly implement basic data security practices.

43. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[18] *Id.*

44. Die to the nature of the information Defendant chose to custody Defendant was at all times fully aware of its obligation to protect the PII consumers. As an entity that custodies PII Defendant was also aware of the significant repercussions that would result from its protect that information from unauthorized access.

Defendant Fails to Comply with HIPAA

45. HIPAA requires covered entities like Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

46. Covered entities (including Defendant) must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

47. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D); and 45 C.F.R. § 164.530(b).

48. A Data Breach such as the one Defendant experienced is also considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

49. Data breaches where an unauthorized individual gains access to PHI are also Security Incidents under HIPAA because they impair both the integrity (data is not interpretable) and availability (data is not accessible) of patient health information:

> The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule. A security incident is defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. See the definition of security incident at 45 C.F.R. 164.304. Once the ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures. See 45 C.F.R.164.308(a)(6).[19]

50. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards and standards of care mandated by HIPAA regulations.

Defendant Fails to Comply with Industry Standards

51. Experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

52. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

[19] *See* https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf at 4.

malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

53. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

54. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

55. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach and the resulting harm to Plaintiff and the Class.

Defendant's Breach

56. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect patients' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption);

o. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and

p. Failing to adhere to industry standards for cybersecurity.

57. As the result of antivirus and malware protection software in dire need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks like the ransomware intrusion here, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access and compromise Defendant's IT systems, which contained unsecured and unencrypted PII.

58. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

Data Breaches Cause Harm and Put Consumers at Risk

59. Data breaches at healthcare related providers like Defendant are especially problematic because the breaches can negatively impact the overall daily lives of individuals affected by the attack.

60. For instance, loss of access to patient histories, charts, images, and other information forces providers to limit or cancel patient treatment because of the disruption of service.

61. This leads to a deterioration in the quality of overall care patients receive at facilities affected by data breaches.

62. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[20]

[20] *See* Nsikan Akpan, Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart- attacks (last visited Jan. 25, 2022).

63. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[21]

64. Similarly, data breach incidents cause patients issues with receiving care that rise above the level of mere inconvenience. The issues that patients encounter as a result of such incidents include, but are not limited to:

a. rescheduling their medical treatment;

b. finding alternative medical care and treatment;

c. delaying or foregoing medical care and treatment;

d. undergoing medical care and treatment without medical providers having access to a complete medical history and records; and

e. inability to access their medical records.[22]

65. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[23]

66. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black

[21] *See* Sung J. Choi et al., Cyberattack Remediation Efforts and Their Implications for Hospital Quality, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Jan. 25, 2022).

[22] *See, e.g.,* Lisa Vaas, Cyberattacks Paralyze, and Sometimes Crush, Hospitals, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals// (last visited Jan. 25, 2022); Jessica David, Data Breaches Will Cost Healthcare $4B in 2019. Threats Outpace Tech, Health IT Security (Nov. 5, 2019), https://healthitsecurity.com/news/data-breaches-will-cost-healthcare-4b-in-2019-threats-outpace-tech - :~:text=November 05, 2019 - Healthcare data,per each breach patient record (last visited Jan. 25, 2022).

[23] *See* U.S. Gov. Accounting Office, GAO-07-737, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" (GOA, 2007). Available at https://www.gao.gov/new.items/d07737.pdf. (last visited Jan. 25, 2022).

market to identity thieves who desire to extort and harass victims, taking over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

67. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[24]

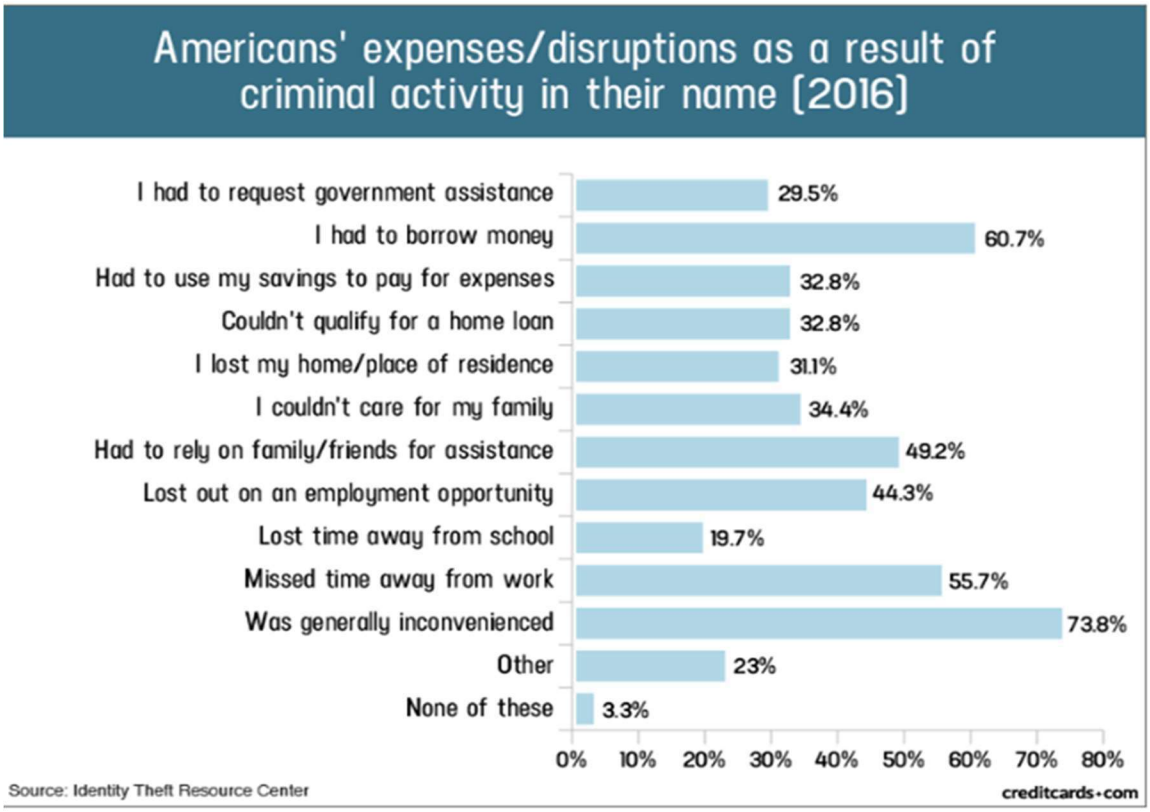
68. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

69. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give

[24] *See* IdentityTheft.gov, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 25, 2022).

the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

70. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[25]



71. Moreover, theft of PII results in the loss of a valuable property right.[26]

72. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

---

[25] *See* Jason Steele, Credit Card and ID Theft Statistics, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. (last visited Jan. 25, 2022).

[26] *See*, e.g., John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

73. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

74. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> *See* GAO Report, at p. 29.

75. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

76. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

77. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

78. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[27] PII is particularly valuable because criminals can use it to target victims

[27] *See* Ashiq Ja, Hackers Selling Healthcare Data in the Black Market, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 25, 2022).

with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

79. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[28] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[29] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

80. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

81. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

82. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

[28] Identity Theft and Your Social Security Number, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 25, 2022).
[29] *Id*. at 4.

83. For this reason, Defendant knew or should have known about these dangers and strengthened its data security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

Plaintiff and Class Members' Damages

84. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

85. Defendant is only providing Plaintiff and Class Members with one year of identity theft protection. After that year concludes, Plaintiff and Class Members will be required to pay for credit monitoring or identity theft protection services out of their own pocket. The cost for credit monitoring to consumers can be as much as $360 per year for many years.[30] Moreover, Defendant's refusal to mitigate the fallout from the Data Breach means that Plaintiff and Class Members will be required to devote more time and effort to remedy the effects than they otherwise must.

86. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

87. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, and similar identity theft.

[30] https://compliancy-group.com/the-hidden-costs-of-a-data-breach/

88. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

89. Plaintiff and Class Members will also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

90. Plaintiff and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant obtained from Plaintiff and Class Members; (b) violation of their privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud; and (d) emotional distress.

91. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

92. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

Plaintiff Ford's Experience

93. Plaintiff Ford's information came into the custody of Defendant and was compromised in the Data Breach.

94. Since the Data Breach, Plaintiff Ford has suffered from fraud as a result of his Social Security number and other PII being compromised in the Data Breach, specifically credit cards have been opened in his name and other loans and other accounts have attempted to be opened.

95. Plaintiff has spent a significant number of hours reviewing his bank accounts, contacting his bank, and contacting other businesses, and will continue to spend valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

96. Additionally, Plaintiff Ford is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

97. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

98. Plaintiff suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of PII, a form of property that Defendant obtained; (b) violation of privacy rights;(c) the likely theft of PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

99. As a result of the Data Breach, Plaintiff has also suffered emotional distress as a result of the release of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

100. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

101. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

102. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

103. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the following nationwide class:

> All persons residing in the United States whose PII and/or PHI was accessed, acquired, used, or disclosed as a result of the Data Breach Defendant revealed on September 9, 2022 ("the Class").

104. Excluded from the Class are Defendant, their subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendant have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

105. Plaintiff reserves the right to modify or amend the definition of the proposed Class, if necessary, before this Court determines whether certification is appropriate.

106. The requirements of Rule 23(a)(1) are satisfied. The Class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective Class Members through this class action will benefit both the parties and this Court. Empress EMS's disclosure to HHS OCR indicates that approximately 318,558 individuals were affected by the Data Breach.

107. The exact size of the Class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the information implicated in the Data Breach.

108. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting Class Members. The questions

of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant had a duty to secure and protect the PII of Plaintiff and Class Members;

b. Whether Defendant were negligent in collecting and disclosing Plaintiff's and Class Members' PII;

c. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

e. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

f. Whether Defendant breached their duties to exercise reasonable care in handling Plaintiff's and Class Members' PII in the manner alleged herein, including failing to comply with industry standards;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

i. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

j. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

109. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of Class Members. The claims of the Plaintiff and Class Members are based on the same legal theories and arise from the same failure by Defendant to safeguard PII. Plaintiff and Class Members each had their PII disclosed by Defendant to an unauthorized third party.

110. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class Members. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation, including data breach litigation. The claims of Plaintiff and Class Members are substantially identical as explained above. While the aggregate damages that may be awarded to the Class Members are likely to be substantial, the damages suffered by the individual Class Members are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

111. Here a class action is superior to other available methods for the fair and efficient adjudication of this controversy. The adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudications of the asserted claims. There will be no difficulty in managing this action as a class action, and the disposition of the claims of the Class members in a single action will provide substantial benefits to all parties and to the Court. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Defendant's violations of law inflicting damages in the aggregate would go un-remedied.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION

NEGLIGENCE

112. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

113. As a condition of any person or entity using the services of Defendant, Class Members are obligated to (or an entity provides) provide Defendant with PII.

114. Defendant's acceptance and maintenance of this information is for its own pecuniary gain and as part of its regular business activities.

115. Plaintiff and Class Members, and the entities that provided said PII on their behalf entrusted this Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

116. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

117. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their consumers' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

118. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

119. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

120. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendant's business as a financial services firm, for which the diligent protection of PII is a continuous forefront issue.

121. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew of should have known of the inherent risks in collecting and storing the PII of Plaintiff and Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

122. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also

included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Defendant.

123. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

124. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

125. Defendant had and continues to have a duty to adequately and promptly disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

126. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

127. Defendant has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

128. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Defendant's possession or control.

129. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for

Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

130. These foregoing frameworks are existing and applicable industry standards in the medical services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

131. Defendant improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

132. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect consumers' PII in the face of increased risk of theft.

133. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its consumers' PII.

134. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

135. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

136. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

137. Defendant's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Defendant and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

138. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare, dental, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

139. Defendant's violation of 45 C.F.R. § 164.530(c)(l) and related HIPAA provisions constitutes negligence *per se*.

140. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

141. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

142. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

143. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

144. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class.

145. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of consumers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Defendant's goods and services they received.

146. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

147. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

SECOND CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

148. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

149. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for medical treatment, inherent to which was the requirement that Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

150. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

151. Through its statements and other conduct, Defendant manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiff's and Class Members' PII.

152. The valid and enforceable implied contracts to provide medical services that Plaintiff and Class Members entered into with Defendant include the promise to protect non-public PII given to Defendant or that Defendant creates on its own from disclosure.

153. When Plaintiff and Class Members provided their PII to Defendant in exchange for medical services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

154. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

155. Plaintiff and Class Members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

156. Under the implied contracts, Defendant promised and was obligated to: (a) provide healthcare services to Plaintiff and Class Members; and (b) protect Plaintiff's and the Class Members' PII: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their PII.

157. Both the provision of medical services and the protection of Plaintiff's and Class Members' PII were material aspects of these implied contracts.

158. On information and belief, the implied contracts for the provision of labor services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' PII—are also believed to be acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's privacy policy.

159. On information and belief, Defendant's express representations memorialize and embody the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

160. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their PII associated with obtaining healthcare private. To customers such as Plaintiff and Class Members, healthcare that does not adhere to industry standard data security protocols to protect PII is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

161. Plaintiff and Class Members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their PII would be safeguarded and protected, or entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

162. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendant, and provided payment for their medical services in exchange for, and, amongst other things, the protection of their PII.

163. Plaintiff and Class Members performed their obligations under the contract.

164. Defendant materially breached its contractual obligation to protect the non-public PII and PHI Defendant gathered when the sensitive information was accessed by unauthorized persons as part of the Data Breach.

165. Defendant materially breached the terms of the implied contracts. Defendant did not maintain the privacy of Plaintiff's and Class Members' PII as evidenced by its notifications of the Data Breach to Plaintiff and approximately 300,000+ Class Members. In particular, Defendant

did not comply with industry standards, consumer expectations, standards of conduct embodied in statutes like HIPAA and Section 5 of the FTCA, or otherwise protect Plaintiff's and the Class Members' PII, as set forth above.

166. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

167. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain, and instead received employment that was of a diminished value to that described in the contracts. Plaintiff and Class Members therefore were damaged in an amount at least equal to the difference in the value of the medical services with data security protection they bargained for and the medical services they actually received.

168. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have worked with Defendant.

169. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their PII, the loss of control of their PII, the present and imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

170. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the hacking incident and Data Breach.

171. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit and identity monitoring to all Class Members.

THIRD CAUSE OF ACTION

VIOLATIONS OF NEW YORK GEN. BUS. LAW 349

172. Plaintiff re-alleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

173. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members Private Information, which was a proximate and direct cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class Members' PII, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify the Plaintiff and Class Members of the Data Breach;

e. Misrepresenting that certain sensitive PII was not accessed during the Data Breach, when it was;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class Members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501-6505.

174. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

175. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers.

176. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and Class Members' rights.

177. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

178. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

179. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid.

180. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

VII. PRAYER FOR RELIEF

181. **WHEREFORE**, Plaintiff, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as

well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2

Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

VIII. JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury.

DATED: October 12, 2022

Respectfully submitted,

s/ Blake Hunter Yagman

Blake Hunter Yagman
byagman@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: 212-594-5300